UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/723,011	11/26/2003	Vincent J. Zimmer	20002/17853	1136

75343 7590 12/04/2008

Hanley, Flight & Zimmerman, LLC
150 S. Wacker Drive
Suite 2100
Chicago, IL 60606

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
12/04/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/723,011	ZIMMER ET AL.	
	Examiner	Art Unit	
	MATTHEW T. HENNING	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 August 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 November 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

This action is in response to the communication filed on 8/20/2008.

DETAILED ACTION

Response to Arguments

Applicants' arguments with respect prior art rejection of claims 1-32 have been considered but are moot in view of the new ground(s) of rejection, necessitated by the newly recited claim limitations.

Regarding the applicants' argument with respect to the "brief summary of the invention", the examiner does not find the argument persuasive. 37 CFR 1.77(b) states "The specification should include the following sections in order: ... (7) Brief summary of the invention." As such, the specification should provide a brief summary of the invention. The applicants argument regarding the MPEP's statement of "when set forth" is not found persuasive. The MPEP states "such summary should, when set forth, be commensurate with the invention as claimed". In other words, at the time that it is set forth, the summary should be commensurate with the invention as claimed. This section does not question the requirement of a brief summary of the invention, but rather indicates that the summary should reflect the claim language present at the time when the summary is set forth. As such, the examiner has maintained the objection to the specification under 37 CFR 1.77(b), as indicated below.

All objections and rejections not set forth below have been withdrawn.

Claims 1-32 have been examined.

Specification

Brief Summary of the Invention: See MPEP § 608.01(d). A brief summary or general statement of the invention as set forth in 37 CFR 1.73. The summary is separate and distinct from the abstract and is directed toward the invention rather than the disclosure as a whole. The summary may point out the advantages of the

invention or how it solves problems previously existent in the prior art (and preferably indicated in the Background of the Invention). In chemical cases it should point out in general terms the utility of the invention. If possible, the nature and gist of the invention or the inventive concept should be set forth. Objects of the invention should be treated briefly and only to the extent that they contribute to an understanding of the invention.

The specification is objected to for failing to provide a Brief Summary of the Invention as required by 37 CFR 1.77(b).

Correction is required. See MPEP Section 608.01(d).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1- 7, 9-15, 16-17, 19-22, and 24-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hind et al. (US Patent Number 6,976,163) hereinafter referred to as Hind, and further in view of TCPA (Technical Overview for EFI).

Regarding claims 1 and 26, Hind disclosed a method of securely configuring a first machine (See Hind Fig. 10 Element 706) in a pre-operating system environment (See Hind Col. 2 Paragraph 2), the method comprising: detecting a message (See Hind Col. 11 Lines 19-31); determining an operating mode of the machine (See Hind Col. 12 Lines 45-63); receiving a configuration update (See Hind Col. 18 Lines 52-56); and updating a machine configuration in a

pre-operating system environment (See Hind Col. 18 Lines 52-56 and Fig. 11), but Hind failed to specifically disclose performing a shared secret key exchange; providing an attestation while the first machine is operating in the pre-operating system environment for use by a second machine to determine whether to send a configuration update to the first machine; or receiving the configuration update when the second machine determines that the attestation is authentic. However, Hind did disclose decryption at the receiving device using a shared secret (See Hind Col. 3 Lines 52-59), and did disclose that firmware updates are distributed to the devices based on an authorization associated with the device, which may be provided, for example, by identifying a serial number, MAC address license key or other identifier associated with the device, and then the firmware update may be provided to the device (See Hind Col. 18 Lines 45-56). Hind also fails to disclose how the authorization is performed.

TCPA teaches a method for providing an attestable identity wherein a platform requests a service of a service provider, the service provider requests a signed trust state from the platform, the platform signs the trust state using an attestation ID key and returns the signed trust state to the service provider, which uses a trusted third party to verify the signature and trust state before providing the service (See TCPA 36-41).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have employed the teachings of TCPA in the firmware updating system of Hind by providing each device with an attestation key and performing the challenge-response processing taught by TCPA before providing the firmware update to each device. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide a

specific means for providing authorization to each device using an identifier of the device, before providing the firmware, where only a generic disclosure of such had been made by Hind.

It further would have been obvious to one of ordinary skill in the art at the time of invention to have performed a shared secret key exchange between the firmware distributor and the updatable device of Hind. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide both devices with the proper key so that proper encryption and decryption could occur.

Regarding claims 9, and 29, Hind disclosed a method of securely conveying a configuration update to a client machine operating in a pre-operating system environment, the method comprising: determining an operating mode of the client machine (See Hind Col. 12 Lines 45-63); receiving an attestation (See Hind Col. 18 Lines 45-52); verifying the attestation (See Hind Col. 18 Lines 45-52); and sending a configuration update to the client machine in a pre-operating system environment (See Hind Col. 18 Lines 52-56), but Hind failed to specifically disclose performing a shared secret key exchange; sending a message to the client to determine whether the client machine supports receiving confirmation updates from a remote source while the client is operating in the pre-operating system environment. However, Hind did disclose decryption at the receiving device using a shared secret (See Hind Col. 3 Lines 52-59), and did disclose that firmware updates are distributed to the devices based on an authorization associated with the device, which may be provided, for example, by identifying a serial number, MAC address license key or other identifier associated with the device, and then the firmware update may be provided to the device (See Hind Col. 18 Lines 45-56). Hind also fails to disclose how the authorization is performed.

TCPA teaches a method for providing an attestable identity wherein a platform requests a service of a service provider, the service provider requests a signed trust state from the platform, the platform signs the trust state using an attestation ID key and returns the signed trust state to the service provider, which uses a trusted third party to verify the signature and trust state before providing the service (See TCPA 36-41).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have employed the teachings of TCPA in the firmware updating system of Hind by providing each device with an attestation key and performing the challenge-response processing taught by TCPA before providing the firmware update to each device. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide a specific means for providing authorization to each device using an identifier of the device, before providing the firmware, where only a generic disclosure of such had been made by Hind.

It further would have been obvious to one of ordinary skill in the art at the time of invention to have performed a shared secret key exchange between the firmware distributor and the updatable device of Hind. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide both devices with the proper key so that proper encryption and decryption could occur.

Regarding claim 19, Hind disclosed an apparatus to securely configure a client machine in a pre-operating system environment, the apparatus comprising: a client machine comprising: a first messaging module configured to detect messages and send messages (See Hind Col. 11 Lines 19-31); an operating mode (See Hind Col. 12 Lines 45-63); and a configuration module configured to update the client's configuration in a pre-operating system

environment (See Hind Col. 18 Lines 52-56); and a server machine comprising: a second messaging module configured to send messages and receive messages (See Hind Col. 11 Lines 19-31); and an update module configured to generate the client configuration update (See Hind Col. 18 Lines 52-56), but Hind failed to specifically disclose the client machine comprising a first key exchange module configured to perform a shared secret key exchange, or the server machine comprising a second key exchange module configured to perform a shared secret key exchange after an attestation has been verified; a trusted platform module configured to provide an attestation while the client machine is operating in the pre-operating system environment for use by a server machine to determine whether to send a client configuration update to the client machine; that the second messaging module was for use in sending a message to the client machine to determine whether the client machine supports receiving configuration updates from the server machine while the client machine is operating in the pre-operating system environment;. However, Hind did disclose decryption at the receiving device using a shared secret (See Hind Col. 3 Lines 52-59), and did disclose that firmware updates are distributed to the devices based on an authorization associated with the device, which may be provided, for example, by identifying a serial number, MAC address license key or other identifier associated with the device, and then the firmware update may be provided to the device (See Hind Col. 18 Lines 45-56). Hind also fails to disclose how the authorization is performed.

TCPA teaches a method for providing an attestable identity wherein a platform requests a service of a service provider, the service provider requests a signed trust state from the platform, the platform signs the trust state using an attestation ID key and returns the signed trust state to

the service provider, which uses a trusted third party to verify the signature and trust state before providing the service (See TCPA 36-41).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have employed the teachings of TCPA in the firmware updating system of Hind by providing each device with an attestation key and performing the challenge-response processing taught by TCPA before providing the firmware update to each device. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide a specific means for providing authorization to each device using an identifier of the device, before providing the firmware, where only a generic disclosure of such had been made by Hind.

It would have been obvious to one of ordinary skill in the art at the time of invention to have provided the client and server of Hind each with a shared secret key exchange module. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide both devices with the proper key so that proper encryption and decryption could occur.

Regarding claims 2, and 27, Hind and TCPA disclosed that the message is sent from a second machine (See Hind Col. 11 Lines 19-31).

Regarding claims 3, and 20, Hind and TCPA disclosed that the operating mode of the first machine comprises at least one of an IT-managed machine or a consumer machine (See Hind Col. 12 Lines 45-63 and Col. 18 Line 59 – Col. 19 Line 3).

Regarding claims 4, 12, and 21, Hind and TCPA disclosed that the attestation comprises at least one of machine identity information and a pseudo-anonymous authentication (See Hind Col. 18 Lines 45-52).

Regarding claim 5, Hind and TCPA disclosed that the pseudo-anonymous authentication is provided by a trusted platform module (See TCPA Pages 40-41).

Regarding claims 6, and 13, Hind and TCPA disclosed that the machine identity information comprises at least one of a serial number, a network name, or a cryptographic representation of hardware registers (See TCPA Pages 40-41).

Regarding claims 7, and 14, Hind and TCPA disclosed that the pseudo-anonymous authentication comprises an Attestation Identity Key (See TCPA Pages 40-41).

Regarding claim 10, Hind and TCPA disclosed the message is to a client machine (See Hind Col. 11 Lines 19-31).

Regarding claim 11, Hind and TCPA disclosed that the operating mode of the client machine comprises at least one of an IT-managed device and a personal device (See Hind Col. 12 Lines 45-63 and Col. 18 Line 59 – Col. 19 Line 3).

Regarding claims 15 and 31, Hind and TCPA disclosed that the attestation is verified by a trusted third party (See TCPA Page 41).

Regarding claims 16, 22, 24, and 28, Hind disclosed that the configuration comprises at least one of a firmware setting, a BIOS setting, or a machine setting (See Hind Col. 18 Lines 45-52).

Regarding claims 17, 25, and 32, Hind and TCPA did not specifically disclose the configuration update being encrypted. However, Hind did disclose the update being provided over a network, and it was well known at the time of invention to encrypt transmissions over a network. Therefore, it would have been obvious to the ordinary person skilled in the art at the time of invention to have encrypted the configuration update of Hind. This would have been

obvious because the ordinary person skilled in the art would have been motivated to protect the update from being intercepted by an illicit party.

Regarding claim 30, Hind and TCPA disclosed instructions stored thereon that, when executed, cause the first machine to send the message via a network connection (See Hind Fig. 10).

Claims 8, 18, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hind and TCPA as applied to claim1, 9, and 19 above, and further in view of Girard (US Patent Number 7,093,124).

Hind and TCPA disclosed updating BIOS and Firmware in a computer, but failed to specifically disclose that updating is adapted to operate in an OS-transparent operating mode with networking support.

Girard teaches a system for updating BIOS and system configurations remotely, and teaches that the use of an agent running in the BIOS, prior to loading the operating system, to perform authentication of a new boot image and to perform the required configuration, provides tamper resistance (See Girard Col. 1 Lines 20-47).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Girard in the firmware updating system of Hind and TCPA by performing the downloading, authentication, and configuration of Hind using an agent within the BIOS which is run prior to loading of the operating system. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide the updating with tamper resistance.

Conclusion

Claims 1-32 have been rejected.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MATTHEW T. HENNING whose telephone number is (571)272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Matthew T Henning/
Examiner, Art Unit 2431

/Christopher A. Revak/
Primary Examiner, Art Unit 2431